

- 10 -

REMARKS

The Examiner has rejected Claims 1, 4-6, 9-10, 13, 19-20, 23, 27-29 and 42-44 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, with respect to Claims 1, 19 and 27, the Examiner has argued that in applicant's claimed technique "wherein the certificate includes a link to a web site describing the virus scanning performed on the e-mail by including a type and a version of a virus scanner..." it is unclear whether it is the certificate or the link to the website that describes virus scanning and that includes a type and version number of a virus scanner. The Examiner has also pointed out that Claim 13 depends on cancelled claim 11. Furthermore, Claims 4-6, 9-10, 20, 23, 28-29 and 42-44 have been rejected by virtue of their dependence on the above rejected claims. Applicant respectfully asserts that each of the independent claims along with Claim 13 have been clarified hereinabove to avoid such rejection.

The Examiner has rejected Claims 1, 4, 6, 9-10, 13, 19-20, 23, 27-29 and 44 under 35 U.S.C. 103(a) as being unpatentable over by AVG (AVG anti-virus) as evidenced AVG Tech, AVG 9, Suffolk-L (<http://archiver.rootsweb.com/th/read/SUFFOLK/1999-05/0927040114>), and Microscopy (Microscopy ListServer Archives, <http://www.msa.microscopy.com/cgi-bin/ReadPrintEmailHTML.pl?filename=9905.txt>, 2nd email) in view of Fisher (U.S. Patent No. 5,311,591) and in further view of Chen et al. (U.S. Patent No. 5,832,208). Applicant respectfully disagrees with such rejection, especially in view of the amendments made to the independent claims.

With respect to each of the independent claims, the Examiner has responded to applicant's arguments with respect to applicant's claimed technique "wherein the certificate includes a link to a web site describing the virus scanning performed on the e-mail by including a type and a version of a virus scanner utilized in scanning the e-mail for viruses." Specifically, the Examiner has argued that Suffolk provides a link above the type and version of the virus scanner. Clearly, only providing a link above the type and

- 11 -

version of the virus scanner located in the e-mail, as in Suffolk, does not teach a “web site describing the virus scanning performed on the e-mail by including a type and a version of a virus scanner,” as claimed by applicant (emphasis added). To emphasize, applicant claims that the web site includes the type and version of a virus scanner utilized, and not merely that the e-mail itself includes such information, as in Suffolk. Furthermore, applicant respectfully asserts that the information on the website in Suffolk is general to the AVG software, and is not a web page specific to the “virus scanning performed on the e-mail,” as claimed by applicant.

Still with respect to each of the independent claims, the Examiner has responded to applicant’s arguments with respect to applicant’s claimed “information for reading a digital signature added to the e-mail if no viruses are found.” In particular, the Examiner has argued that “the feature of checking whether a code (program, message, etc.) has been tampered with would be an ideal addition to AVG product especially since it takes time from the completion of scanning e-mail to reception of e-mail by the designated recipient.” Applicant notes, however, that Fischer teaches a manufacturer that signs a program with a digital certificate so that it can be determined “whether or not the program is exactly the same as it was when it was generated by the manufacturer.”

Thus, in Fischer, the digital certificate is only added upon generation of the program by the manufacturer, which inherently assumes that the manufacturer is trusted. Applicant, on the other hand, claims “a digital signature added to the e-mail if no viruses are found” during the scanning of the email, or, in other words, after scanning the email (see the context of applicant’s claims). Thus, applicant’s claim language allows for adding a digital signature based on scanning, and not based on whether the sender of the e-mail is trusted. Applicant respectfully asserts that adding a digital signature upon generation of an e-mail, as Fischer suggests, would defeat applicant’s claimed feature, namely to attach “a certificate identifying the e-mail as being scanned for viruses” where the “certificate includes a link to a web site...including...information for reading a digital signature added to the e-mail if no viruses are found” (emphasis added).

- 12 -

Again, applicant respectfully asserts that the digital signature in Fischer is added to a software program by a manufacturer to prove authenticity so that a current digital signature may be compared with the original digital signature added by the manufacturer at a later date, in order to see if the program has been tampered with. Clearly, the digital signature in Fischer is not added to the program in response to a clean result of a virus scan, in the manner claimed by applicant, but is only added to authenticate the original product.

Furthermore, the Examiner has responded to applicant's arguments with respect to applicant's claimed technique "wherein attaching the certificate comprises attaching the certificate at the server" (see the same or similar, but not necessarily identical language in each of the independent claims). Specifically, the Examiner has relied on AVG in view of Fischer in arguing that the "certificate is attached at the computer that handles the e-mail" and that "Chen teaches an e-mail server handling scanning and sending e-mail."

Applicant respectfully asserts that simply nowhere in AVG is there any disclosure that the "certificate is attached at the computer that handles the e-mail," as argued by the Examiner. In fact, AVG only generally states that "AVG can certify (add a small signature message) to the end of every e-mail" (see AVG 9). After careful review of AVG, applicant notes that AVG is located on the user computer. In particular, AVG teaches downloading update files to a user computer for use in scanning (see AVG Anti-Virus-Free Updates). Thus, in AVG the "computer that handles the e-mail," as the Examiner argues, is the user computer. Thus, even if AVG taught that the certificate was attached at the computer that handled the e-mail, then according to AVG the certificate would be attached at the user computer, and not "at the server," as claimed by applicant.

The Examiner has also argued that "even if the computer were not to be consider[ed] as a server, some kind of server that handles e-mail delivery is inherently necessary in e-mail exchange between a sender and recipient." Clearly, simply because some sort of server must inherently be used in e-mail exchange does not even suggest a

- 13 -

certificate, let alone that “attaching the certificate comprises attaching the certificate at the server,” as claimed by applicant.

Even still yet with respect to each of the independent claims, the Examiner has responded to applicant’s arguments regarding applicant’s claimed technique “wherein the virus scanner is incorporated within a mail application that is utilized in creating the e-mail” (see the same or similar, but not necessarily identical language in each of the independent claims). The Examiner has stated that “[a]lthough AVG does not explicitly teach incorporating the virus scanner with a mail application that is utilized in creating the e-mail, AVG does teach compatibility with MS Outlook clients and Exchange clients” and that “the AVG’s product in addition to be[ing] compatible it also complements e-mail applications.” From such, the Examiner has concluded that “it would have been obvious to one of ordinary skill in the art at the time of applicant’s invention to incorporate the virus scanner within an e-mail application” and that the motivation would have been “to scan and certify e-mails handled by the application as virus free.”

Applicant respectfully disagrees with the Examiner’s assertion. Applicant respectfully asserts that it would not be necessary to incorporate the virus scanner within an e-mail application in order to scan and certify e-mails handled by the application as being virus free, which is clearly evidence by AVG. AVG teaches scanning and certifying e-mails even though the scanner is not incorporated within the mail application. Thus, since the motivation relied on by the Examiner is clearly deficient of providing any real need for incorporating a virus scanner within a mail application, in the specific manner claimed by applicant, it would not have been obvious to modify AVG to meet applicant’s specific claim language.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable

- 14 -

expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, for at least the reasons noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has included the following highlighted claim language in each of the independent claims:

"wherein the certificate includes a link to a web site, the web site describing the virus scanning performed on the e-mail by including a type and a version of a virus scanner utilized in scanning the e-mail for viruses, in addition to information on obtaining digital signature verification software that can be utilized for reading a digital signature added to the e-mail if no viruses are found;

wherein the computer is a network server;

wherein attaching the certificate comprises attaching the certificate at the server;

wherein the virus scanner is incorporated within a mail application that is utilized in creating the e-mail;

wherein the email received at the recipient computer displays the certificate and only displays the digital signature if the digital signature verification software is installed on the recipient computer" (see the same or similar, but not necessarily identical language in each of the independent claims).

Applicant respectfully asserts that simply nowhere in the references relied on by the Examiner is there any disclosure of information on a web page for "obtaining digital signature verification software that can be utilized for reading a digital signature added to

- 15 -

the e-mail if no viruses are found” as presently claimed by applicant (emphasis added). In addition, such references also fail to teach that “the email...only displays the digital signature if the digital signature verification software is installed on the recipient computer,” as presently claimed by applicant (emphasis added).

Again, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Still yet, applicant brings to the Examiner’s attention the subject matter of new Claims 46-49 below, which are added for full consideration:

“wherein the certificate is a water marked seal” (see Claim 46);

“wherein the digital signature verification software is incorporated within the mail application for reading digital signatures included in received e-mails” (see Claim 47);

“wherein the digital signature verification software is incorporated within the virus scanner for reading digital signatures included in received e-mails” (see Claim 48); and

“wherein the e-mail received at the recipient computer only displays the digital signature if the digital signature verification software is installed on the recipient computer and if the digital signature verification software verifies the digital signature” (see Claim 49).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

- 16 -

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P140/01.131.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100